Сложность пропозициональных доказательств

Эдуард Алексеевич Гирш

http://logic.pdmi.ras.ru/~hirsch

ПОМИ РАН

28 октября 2010 г.

Принцип Дирихле

Нижняя оценка $\Omega(n)$ на ширину вывода

- Сократим ширину аксиом: “забудем” о некоторых возможностях.
- G-PHP: двудольный граф G задаёт возможности размещения.

- Сократим ширину аксиом: "забудем" о некоторых возможностях.
- G-PHP: двудольный граф G задаёт возможности размещения.
- Пусть $G = ((P, H), E)$ — двудольный расширитель: степень — константа, имеются константы $\epsilon, \rho \in (0; 1)$, т.ч.
$$\forall P' \subseteq P \ (|P'| \leq \rho|P| \Rightarrow |\partial P'| \geq \epsilon|P'|),$$
где $\partial P'$ — те клетки, где может сидеть ровно один кролик из P'.

- Сократим ширину аксиом: "забудем" о некоторых возможностях.
- G-PHP: двудольный граф G задаёт возможности размещения.
- Пусть $G = ((P, H), E)$ — двудольный расширитель: степень — константа, имеются константы $\epsilon, \rho \in (0; 1)$, т.ч.

$$\forall P' \subseteq P \ (|P'| \leq \rho |P| \Rightarrow |\partial P'| \geq \epsilon |P'|),$$

  где $\partial P'$ — те клетки, где может сидеть ровно один кролик из P'.
- "Уравнения" кролика p

$$\left(\bigvee_{(p,h) \in E} x_{ph} \right) \wedge \bigwedge_{\substack{(p,h),(p',h) \in E \\ p \neq p'}} (\neg x_{ph} \vee \neg x_{p'h}).$$

Принцип Дирихле

Нижняя оценка $\Omega(n)$ на ширину вывода

- Сократим ширину аксиом: “забудем” о некоторых возможностях.
- G-PHP: двудольный граф G задаёт возможности размещения.
- Пусть $G = ((P, H), E)$ — двудольный расширитель: степень — константа, имеются константы $\epsilon, \rho \in (0; 1)$, т.ч.

$$\forall P' \subseteq P \; (|P'| \leq \rho |P| \Rightarrow |\partial P'| \geq \epsilon |P'|),$$

  где $\partial P'$ — те клетки, где может сидеть ровно один кролик из P'.
- “Уравнения” кролика p

$$\left(\bigvee_{(p,h) \in E} x_{ph} \right) \wedge \bigwedge_{\substack{(p,h),(p',h) \in E \\ p \neq p'}} (\neg x_{ph} \vee \neg x_{p'h}).$$

- Любые $\rho|P|$ уравнений совместны; все $|P|$ — нет.
- В выводе есть дизъюнкция C, следующая в точности из уравнений для множества P' размером $\in \left[\frac{1}{3}\rho|P| \,..\, \frac{2}{3}\rho|P|\right]$.

- Сократим ширину аксиом: “забудем” о некоторых возможностях.
- G-PHP: двудольный граф G задаёт возможности размещения.
- Пусть $G = ((P, H), E)$ — двудольный расширитель: степень — константа, имеются константы $\epsilon, \rho \in (0; 1)$, т.ч.
$$\forall P' \subseteq P \ (|P'| \leq \rho|P| \Rightarrow |\partial P'| \geq \epsilon|P'|),$$
где $\partial P'$ — те клетки, где может сидеть ровно один кролик из P'.
- “Уравнения” кролика p
$$\left(\bigvee_{(p,h)\in E} x_{ph}\right) \wedge \bigwedge_{\substack{(p,h),(p',h)\in E \\ p\neq p'}} (\neg x_{ph} \vee \neg x_{p'h}).$$
- Любые $\rho|P|$ уравнений совместны; все $|P|$ — нет.
- В выводе есть дизъюнкция C, следующая в точности из уравнений для множества P' размером $\in \left[\frac{1}{3}\rho|P| \, .. \, \frac{2}{3}\rho|P|\right]$.
- Для каждой клетки из $\partial P'$ в C должна быть переменная.

Корректность метода резолюций (Reflection)

- Корректность системы док-в Π — невыполнимость формул

$$\Pi(x, y) = 1 \ \wedge \ x[z] = 1$$

(для конкретного размера формулы x, набора значений z, док-ва y).

Корректность метода резолюций (Reflection)

- Корректность метода резолюций — невыполнимость формул

$$\mathrm{Res}(x, y) = 1 \;\wedge\; x[z] = 1$$

  (для конкретного размера формулы x, набора значений z, док-ва y).
- В Res нет коротких док-в корректности Res.

Корректность метода резолюций (Reflection)

- Корректность метода резолюций — невыполнимость формул

$$\mathrm{Res}(x, y) = 1 \;\wedge\; x[z] = 1$$

(для конкретного размера формулы x, набора значений z, док-ва y).

- В Res нет коротких док-в корректности Res.
- Res(2): Res с новыми переменными для 2-конъюнкций:

$$\neg a_{x,y} \vee x, \qquad \neg a_{x,y} \vee y, \qquad \neg x \vee \neg y \vee a_{x,y}.$$

- В Res(2) есть короткие док-ва корректности Res.

Корректность метода резолюций (Reflection)

- Корректность метода резолюций — невыполнимость формул

$$\mathrm{Res}(x, y) = 1 \ \wedge \ x[z] = 1$$

(для конкретного размера формулы x, набора значений z, док-ва y).

- В Res нет коротких док-в корректности Res.
- Res(2): Res с новыми переменными для 2-конъюнкций:

$$\neg a_{x,y} \vee x, \qquad \neg a_{x,y} \vee y, \qquad \neg x \vee \neg y \vee a_{x,y}.$$

- В Res(2) есть короткие док-ва корректности Res.
- ...и корректности Res(2).

Корректность метода резолюций

Точная формулировка: переменные

- Индексы:
  - Формула от n переменных (индексы $v \in [1\,..\,n]$).
  - $\ldots$ из m дизъюнкций (индексы $\ell \in [1\,..\,m]$).
  - Вывод из r дизъюнкций (индексы $\ell \in [1\,..\,r]$).
  - Отрицания указываются индексами $b \in \{0, 1\}$.

Корректность метода резолюций

Точная формулировка: переменные

- Индексы:
  - Формула от n переменных (индексы $v \in [1\,..\,n]$).
  - …из m дизъюнкций (индексы $\ell \in [1\,..\,m]$).
  - Вывод из r дизъюнкций (индексы $\ell \in [1\,..\,r]$).
  - Отрицания указываются индексами $b \in \{0, 1\}$.
- Формула — таблица вхождений $x_{\ell,v,b}$.

- Индексы:
  - Формула от n переменных (индексы $v \in [1\,..\,n]$).
  - ...из m дизъюнкций (индексы $\ell \in [1\,..\,m]$).
  - Вывод из r дизъюнкций (индексы $\ell \in [1\,..\,r]$).
  - Отрицания указываются индексами $b \in \{0, 1\}$.
- Формула — таблица вхождений $x_{\ell,v,b}$.
- Набор — значения z_v и указатели $z_{\ell,v,b}$ (что вып. ℓ ?).

Корректность метода резолюций

Точная формулировка: переменные

- Индексы:
  - Формула от n переменных (индексы $v \in [1\,..\,n]$).
  - …из m дизъюнкций (индексы $\ell \in [1\,..\,m]$).
  - Вывод из r дизъюнкций (индексы $\ell \in [1\,..\,r]$).
  - Отрицания указываются индексами $b \in \{0, 1\}$.
- Формула — таблица вхождений $x_{\ell,v,b}$.
- Набор — значения z_v и указатели $z_{\ell,v,b}$ (что вып. ℓ ?).
- Док-во —
  - дизъюнкции $y_{\ell,v,b}$,
  - зависимости $p_{\ell,\ell',b}$: дизъюнкция ℓ получена резольвированием ℓ', b — знак резольвируемой переменной,
  - резольвируемая переменная $w_{\ell,v}$.

Корректность метода резолюций

Точная формулировка: дизъюнкции

- Каждая дизъюнкция чем-то выполнена: $\bigvee_{v,b} z_{\ell,v,b}$.
- Тем, что *есть* в ней: $\neg z_{\ell,v,b} \vee x_{\ell,v,b}$.
- Набор согласован с указателями: $\neg z_{\ell,v,0} \vee z_v, \quad \neg z_v \vee \neg z_{\ell,v,1}$.

Корректность метода резолюций

Точная формулировка: дизъюнкции

- Каждая дизъюнкция чем-то выполнена: $\bigvee\limits_{v,b} z_{\ell,v,b}$.
- Тем, что *есть* в ней: $\neg z_{\ell,v,b} \vee x_{\ell,v,b}$.
- Набор согласован с указателями: $\neg z_{\ell,v,0} \vee z_v, \quad \neg z_v \vee \neg z_{\ell,v,1}$.
- Формула — часть вывода: $\neg x_{\ell,v,b} \vee y_{\ell,v,b}$.

Корректность метода резолюций

Точная формулировка: дизъюнкции

- Каждая дизъюнкция чем-то выполнена: $\bigvee_{v,b} z_{\ell,v,b}$.
- Тем, что *есть* в ней: $\neg z_{\ell,v,b} \vee x_{\ell,v,b}$.
- Набор согласован с указателями: $\neg z_{\ell,v,0} \vee z_v, \quad \neg z_v \vee \neg z_{\ell,v,1}$.

- Формула — часть вывода: $\neg x_{\ell,v,b} \vee y_{\ell,v,b}$.
- Для надёжности, $\neg y_{\ell,v,0} \vee \neg y_{\ell,v,1}$.

Корректность метода резолюций

Точная формулировка: дизъюнкции

- Каждая дизъюнкция чем-то выполнена: $\bigvee_{v,b} z_{\ell,v,b}$.
- Тем, что *есть* в ней: $\neg z_{\ell,v,b} \vee x_{\ell,v,b}$.
- Набор согласован с указателями: $\neg z_{\ell,v,0} \vee z_v, \quad \neg z_v \vee \neg z_{\ell,v,1}$.

- Формула — часть вывода: $\neg x_{\ell,v,b} \vee y_{\ell,v,b}$.
- Для надёжности, $\neg y_{\ell,v,0} \vee \neg y_{\ell,v,1}$.
- ℓ не с потолка упало: $\bigvee_{\ell'<\ell} p_{\ell,\ell',b}, \quad \bigvee_{v} w_{\ell,v}$.

Корректность метода резолюций

Точная формулировка: дизъюнкции

- Каждая дизъюнкция чем-то выполнена: $\bigvee_{v,b} z_{\ell,v,b}$.
- Тем, что *есть* в ней: $\neg z_{\ell,v,b} \vee x_{\ell,v,b}$.
- Набор согласован с указателями: $\neg z_{\ell,v,0} \vee z_v, \quad \neg z_v \vee \neg z_{\ell,v,1}$.

- Формула — часть вывода: $\neg x_{\ell,v,b} \vee y_{\ell,v,b}$.
- Для надёжности, $\neg y_{\ell,v,0} \vee \neg y_{\ell,v,1}$.
- ℓ не с потолка упало: $\bigvee_{\ell'<\ell} p_{\ell,\ell',b}, \quad \bigvee_{v} w_{\ell,v}$.
- Резольвента по *одной* переменной: $\neg w_{\ell,v} \vee \neg w_{\ell,v'}$.

Корректность метода резолюций

Точная формулировка: дизъюнкции

- Каждая дизъюнкция чем-то выполнена: $\bigvee_{v,b} z_{\ell,v,b}$.
- Тем, что *есть* в ней: $\neg z_{\ell,v,b} \vee x_{\ell,v,b}$.
- Набор согласован с указателями: $\neg z_{\ell,v,0} \vee z_v, \quad \neg z_v \vee \neg z_{\ell,v,1}$.

- Формула — часть вывода: $\neg x_{\ell,v,b} \vee y_{\ell,v,b}$.
- Для надёжности, $\neg y_{\ell,v,0} \vee \neg y_{\ell,v,1}$.
- ℓ не с потолка упало: $\bigvee_{\ell'<\ell} p_{\ell,\ell',b}, \quad \bigvee_{v} w_{\ell,v}$.
- Резольвента по *одной* переменной: $\neg w_{\ell,v} \vee \neg w_{\ell,v'}$.
- Которая *была*: $\neg w_{\ell,v} \vee \neg p_{\ell,\ell',b} \vee y_{\ell',v,b}$.

Корректность метода резолюций

Точная формулировка: дизъюнкции

- Каждая дизъюнкция чем-то выполнена: $\bigvee_{v,b} z_{\ell,v,b}$.
- Тем, что *есть* в ней: $\neg z_{\ell,v,b} \vee x_{\ell,v,b}$.
- Набор согласован с указателями: $\neg z_{\ell,v,0} \vee z_v, \quad \neg z_v \vee \neg z_{\ell,v,1}$.

- Формула — часть вывода: $\neg x_{\ell,v,b} \vee y_{\ell,v,b}$.
- Для надёжности, $\neg y_{\ell,v,0} \vee \neg y_{\ell,v,1}$.
- ℓ не с потолка упало: $\bigvee_{\ell'<\ell} p_{\ell,\ell',b}, \quad \bigvee_{v} w_{\ell,v}$.
- Резольвента по *одной* переменной: $\neg w_{\ell,v} \vee \neg w_{\ell,v'}$.
- Которая *была*: $\neg w_{\ell,v} \vee \neg p_{\ell,\ell',b} \vee y_{\ell',v,b}$.
- Остальные переменные на месте: $\neg p_{\ell,\ell',b} \vee \neg w_{\ell,v} \vee \neg y_{\ell',v,b'} \vee y_{\ell,v,b}$.

Корректность метода резолюций

Точная формулировка: дизъюнкции

- Каждая дизъюнкция чем-то выполнена: $\bigvee_{v,b} z_{\ell,v,b}$.
- Тем, что *есть* в ней: $\neg z_{\ell,v,b} \vee x_{\ell,v,b}$.
- Набор согласован с указателями: $\neg z_{\ell,v,0} \vee z_v, \quad \neg z_v \vee \neg z_{\ell,v,1}$.

- Формула — часть вывода: $\neg x_{\ell,v,b} \vee y_{\ell,v,b}$.
- Для надёжности, $\neg y_{\ell,v,0} \vee \neg y_{\ell,v,1}$.
- ℓ не с потолка упало: $\bigvee_{\ell'<\ell} p_{\ell,\ell',b}, \quad \bigvee_{v} w_{\ell,v}$.
- Резольвента по *одной* переменной: $\neg w_{\ell,v} \vee \neg w_{\ell,v'}$.
- Которая *была*: $\neg w_{\ell,v} \vee \neg p_{\ell,\ell',b} \vee y_{\ell',v,b}$.
- Остальные переменные на месте: $\neg p_{\ell,\ell',b} \vee \neg w_{\ell,v} \vee \neg y_{\ell',v,b'} \vee y_{\ell,v,b}$.
- «В общем, все умерли»: $\neg y_{\ell,v,b}$.

Последовательно доказываем, что выполняющий набор z выполняет все дизъюнкции вывода y, включая последнюю (пустую):

$$\bigvee_{v} (y_{\ell,v,0} \wedge z_v) \vee (y_{\ell,v,1} \wedge \neg z_v).$$

Последовательно доказываем, что выполняющий набор z выполняет все дизъюнкции вывода y, включая последнюю (пустую):

$$\bigvee_v (y_{\ell,v,0} \wedge z_v) \vee (y_{\ell,v,1} \wedge \neg z_v).$$

- Доказываем при условии $p_{\ell,\ell',0}$, $p_{\ell,\ell'',1}$, $w_{\ell,v}$, когда-нибудь потом воспользуемся существованием ℓ', ℓ'', v.

Последовательно доказываем, что выполняющий набор z выполняет все дизъюнкции вывода y, включая последнюю (пустую):

$$\bigvee_{v}(y_{\ell,v,0} \wedge z_v) \vee (y_{\ell,v,1} \wedge \neg z_v).$$

- Доказываем при условии $p_{\ell,\ell',0}$, $p_{\ell,\ell'',1}$, $w_{\ell,v}$, когда-нибудь потом воспользуемся существованием ℓ', ℓ'', v.
- Уцелевшие переменные наследуются из резольвированных д., модифицируем старые д. в новую.

Последовательно доказываем, что выполняющий набор z выполняет все дизъюнкции вывода y, включая последнюю (пустую):

$$\bigvee_v (y_{\ell,v,0} \wedge z_v) \vee (y_{\ell,v,1} \wedge \neg z_v).$$

- Доказываем при условии $p_{\ell,\ell',0}$, $p_{\ell,\ell'',1}$, $w_{\ell,v}$, когда-нибудь потом воспользуемся существованием ℓ', ℓ'', v.
- Уцелевшие переменные наследуются из резольвированных д., модифицируем старые д. в новую.
- Пропавшая явно указывает, какой из членов $\vee$ выполнен (знаем знак переменной), остаётся z_v (а для другой — $\neg z_v$, осталось срезольвировать).

- Короткое док-во $\mapsto$ маленькая монотонная схема, отделяющая выполнимые формулы от имеющих короткие док-ва.

- Короткое док-во $\mapsto$ маленькая монотонная схема, отделяющая выполнимые формулы от имеющих короткие док-ва.
- Отделим k-раскрашиваемые графы от содержащих k^2-клику.

Теорема (Alon, Boppana)

$3 \le k \le K$ и $K\sqrt{k} \le m/(8\log m) \implies$ монотонные схемы, отделяющие k-раскрашиваемые графы с m вершинами от содержащих K-клики, имеют размер $\ge \frac{1}{8}\left(\frac{m}{4K\sqrt{k}\log m}\right)^{(\sqrt{k}+1)/2}$.

Осталось извлечь схему для раскрашиваемости из доказательств для Reflection.

- Короткое док-во $\mapsto$ маленькая монотонная схема, отделяющая выполнимые формулы от имеющих короткие док-ва.
- Отделим k-раскрашиваемые графы от содержащих k^2-клику. Граф $G \mapsto$ формула F о k-раскрашиваемости + доп. переменные для всех конъюнкций длины $(\log n)^{O(1)}$.

- Короткое док-во $\mapsto$ маленькая монотонная схема, отделяющая выполнимые формулы от имеющих короткие док-ва.
- Отделим k-раскрашиваемые графы от содержащих k^2-клику. Граф $G \mapsto$ формула F о k-раскрашиваемости + доп. переменные для всех конъюнкций длины $(\log n)^{O(1)}$.
- В первом случае F выполнима.

- Короткое док-во $\mapsto$ маленькая монотонная схема, отделяющая выполнимые формулы от имеющих короткие док-ва.
- Отделим k-раскрашиваемые графы от содержащих k^2-клику.
  Граф $G \mapsto$ формула F о k-раскрашиваемости + доп. переменные для всех конъюнкций длины $(\log n)^{O(1)}$.
- В первом случае F выполнима.
- Во втором случае F имеет "короткое" док-во невыполнимости:
  - среди её дизъюнкций есть принцип Дирихле $k^2 \mapsto k$;
  - у него есть док-во размера $2^{(\log n)^{O(1)}}$ в $\mathrm{Res}((\log n)^{O(1)})$:

Корректность метода резолюций

Нижняя оценка для метода резолюций

- Короткое док-во $\mapsto$ маленькая монотонная схема, отделяющая выполнимые формулы от имеющих короткие док-ва.
- Отделим k-раскрашиваемые графы от содержащих k^2-клику. Граф $G \mapsto$ формула F о k-раскрашиваемости + доп. переменные для всех конъюнкций длины $(\log n)^{O(1)}$.
- В первом случае F выполнима.
- Во втором случае F имеет "короткое" док-во невыполнимости:
  - среди её дизъюнкций есть принцип Дирихле $k^2 \mapsto k$;
  - у него есть док-во размера $2^{(\log n)^{O(1)}}$ в $\mathrm{Res}((\log n)^{O(1)})$:
    - разделим кроликов на k стай по k штук, клетки на 2 по $k/2$ штук, какая-то стая целиком в первой клетке $\implies$ инъекция $k \mapsto \frac{k}{2}$; иначе каждая даёт кролика во вторую $\implies$ инъекция $k \mapsto \frac{k}{2}$.
    - композиция инъекций $k^2 \mapsto k$, $k \mapsto \frac{k}{2}$ даёт $k^2 \mapsto \frac{k}{2}$.
    - повторим $\log k$ раз.

- Короткое док-во $\mapsto$ маленькая монотонная схема, отделяющая выполнимые формулы от имеющих короткие док-ва.
- Отделим k-раскрашиваемые графы от содержащих k^2-клику. Граф $G \mapsto$ формула F о k-раскрашиваемости + доп. переменные для всех конъюнкций длины $(\log n)^{O(1)}$.
- В первом случае F выполнима.
- Во втором случае F имеет "короткое" док-во невыполнимости:
  - среди её дизъюнкций есть принцип Дирихле $k^2 \mapsto k$;
  - у него есть док-во размера $2^{(\log n)^{O(1)}}$ в $\mathrm{Res}((\log n)^{O(1)})$:
    - разделим кроликов на k стай по k штук, клетки на 2 по $k/2$ штук, какая-то стая целиком в первой клетке $\implies$ инъекция $k \mapsto \frac{k}{2}$; иначе каждая даёт кролика во вторую $\implies$ инъекция $k \mapsto \frac{k}{2}$.
    - композиция инъекций $k^2 \mapsto k$, $k \mapsto \frac{k}{2}$ даёт $k^2 \mapsto \frac{k}{2}$.
    - повторим $\log k$ раз.

Упражнение

Доделать док-во принципа Дирихле $k^2 \mapsto k$ в $Res((\log k)^{O(1)})$.

- Короткое док-во $\mapsto$ маленькая монотонная схема, отделяющая выполнимые формулы от имеющих короткие док-ва.

Корректность метода секущих плоскостей

Нижняя оценка для CP

- Короткое док-во $\mapsto$ маленькая монотонная схема, отделяющая выполнимые формулы от имеющих короткие док-ва.
- Отделим k-раскрашиваемые графы от содержащих $(k+1)$-клику.
- Дальнейшее аналогично резолюции, только проще: обычный принцип Дирихле имеет короткие док-ва в CP!

Корректность метода секущих плоскостей

Нижняя оценка для CP

- Короткое док-во $\mapsto$ маленькая монотонная схема, отделяющая выполнимые формулы от имеющих короткие док-ва.
- Отделим k-раскрашиваемые графы от содержащих $(k+1)$-клику.
- Дальнейшее аналогично резолюции, только проще:
  обычный принцип Дирихле имеет короткие док-ва в CP!
- Осталось сформулировать корректность CP — ясно, что это можно сделать, сохранив условие на монотонность вхождений переменных формулы, ведь
  - обе части действительно монотонно от них зависят,
  - а остальное делается так же, как в док-ве теоремы Кука-Левина об **NP**-полноте SAT.